Date: Thu, 20 Apr 2000 11:04:27 -0700
From: "Jon C. Graff" <jongraff@earthlink.net>
X-Mailer: Mozilla 4.5 [en] (Win98; U)
X-Accept-Language: en
To: AESround2@nist.gov
CC: Mike Battistel <batfamly@netcom.ca>, Kevin Collins <collike@earthlink.net>,
Eric Ashdown <eashdown@earthlink.net>,
Steven A Dougherty <cybercop89@juno.com>,
Noel Lawler <nflawler@aol.com>, Bill Willis <BFWillis1@aol.com>,
Dave Anderson <danderson31@earthlink.net>,
"Gilmore, Pat" <Pat.Gilmore@Schwab.COM>,
Harry DeMaio <hdemaio@dttus.com>
Subject: Selection of the AES finalist

Please see the attachment.

Jon Graff

MEMO

To: NIST AES
From: Jon Graff
Date: April 20, 2000
Subject: Considerations in selecting the final AES algorithm

1. There should only be one algorithm designated as for the AES.

   A second may be indicated as a potential backup in the case of an intellectual property attack, i.e., a "stealth" patent attack. This second algorithm should not be considered as a standard, should NOT be implemented as part of the standard and should only be kept within the first 5 year review cycle.

   A. I agree with Adi Shimar's comments on the need for a single algorithm selection. As he stated, if any of the 5 finalists are "cracked", it will be by a new attack that will quite likely invalidate the other 4. Thus there will be a need to open a new investigation and search for a replacement.

   B. I strongly believe that only ONE algorithm should be chosen for security reasons. It is hard enough to implement a single cryptographic system correctly. Having to deal with two possible algorithms greatly increases the complexity of implementations and therefore significantly increases the likelihood of security flaws.

      As one example of the added complexity and security risks of having two AES algorithms, if there are two algorithms, implementers will have to have "translation" sites where something encrypted under one algorithm must be translated into the second. This translation process may cause for the creation of at least temporarily exposed plaintext. This exposure is a particularly worrisome consideration because many implementations will be done in software, not in protected hardware cryptographic modules.

   C. Because only one AES algorithm should be selected, I believe that certain security safeguards should be kept in place.

      1) The 5 year review cycle should be kept and maintained, and enhanced. At each 5 year review the AES should be reviewed with not only whether it should be re-certified, but also whether its replacement process should be started. Based on what we now know about DES and its viability, the selection process for AES might well have been started 5 years earlier than it did.

      2) The triple DES standards should be rapidly converted to algorithm "agnostic" standards, so that if necessary, if the AES is becomes cryptographically weakened, the triple AES option should be readily available without

prolonged debates and going through the standardization process. This will give some "breathing room" to start a search for an AES replacement (i.e., the MAES, the More Advanced Encryption Standard).

2. If NIST believes that all 5 candidates are cryptographically strong, I believe that as part of the announcement process that NIST should state so. This rewards the "runner's up" for their efforts and contributions.

   Indeed, based on the information submitted, it may not be possible to select one algorithm over the others for any significant reason or justification. NIST may have to make the choice for "esthetic" reasons that are not entirely rational. If there is truly are no discernable differences, perhaps NIST should have a drawing of the contestants from the famed and often cited statistical "urn" filled with balls each containing a single algorithm's name. I would recommend that this ceremony could take place publicly under the additional supervision of the International Association for Cryptographic Research (IACR) at Crypto' 2000 in Santa Barbara this summer.

Sincerely,

Jon Graff